Mobile Application Security Assessment – Service Description

This Service Description describes Mobile Application Security Assessment ("**Service**"). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below).

This Service Description is part of and incorporated into, as applicable: (i) Customer's manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at https://www.sophos.com/legal (collectively referred to as the "**Agreement**"). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to https://www.sophos.com/legal.

1.1 Overview

Sophos will conduct a mobile application security assessment as defined in this Service Description. To help reduce Customer's overall risks and associated remediation costs, Sophos will use a holistic and prioritized approach that assesses the security and compliance risks of the entire mobile application, its associated internal or Internet systems, and the interactions between them. Specific techniques used during the assessment will vary based on mobile platform, purpose of the mobile application, coding practices and quality of the mobile application, and the unique deployment environment.

1.2 Customer Obligations

Customer will perform the standard obligations listed below, and acknowledges and agrees that the ability of Sophos to perform the Service is contingent upon the following:

- Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Sophos, to permit Sophos to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- This service is delivered remotely, but exceptions can be requested. Sophos will evaluate these requests, and if approved for on-site activities, Customer will provide a suitable workspace for Sophos personnel, and necessary access to systems, network, and devices. Sophos reserves the right to deny any and all on-site travel requests.
- Replies to all requests are prompt and in accordance with the delivery dates established between the parties.
- Customer's scheduled interruptions and maintenance intervals allow adequate time for Sophos to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Sophos testing activities as needed, to prevent disruption to Sophos business and performance of the Service (e.g., takedown requests, ISP deny list).
- Customer will provide to Sophos all required information (key personnel contact information, credentials, and related information) at least two (2) weeks before initiating the Service.

The following Customer obligations are specific to the Mobile Application Security Assessment Service:

- Upon commencement of the engagement, Customer will ensure that in-scope applications remain available and stable and will not modify the applications in any way during the course of the engagement. Should any modifications occur during the engagement, Sophos will not consider any changes during testing and reporting and may require a change order and additional fees if modifications result in the need for testing be restarted.
- Customer will ensure that testing the in-scope application, in its configured state, is allowed through any third-party Terms of Service (e.g., AWS and Azure cloud services), especially cloud load-balancing services.

1.3 Scheduling

Sophos will contact a Customer-designated representative within five (5) business days after the execution of an Agreement to begin the Service Initiation activities described herein. These activities will ensure effective and efficient use of the Service.

Sophos will use commercially reasonable efforts to meet Customer's requests for dates and times to deliver the Service(s), taking into consideration Customer-designated downtime windows, Customer deliverable deadlines, and other Customer scheduling requests. Written confirmation of an agreed-upon schedule shall constitute formal acceptance of such schedule.

If an exception for on-site work is approved, and scheduling of any on-site work at Customer facility has been mutually agreed to, any changes by Customer to the on-site work within two (2) weeks of the on-site work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Sophos.

1.4 Timeline

- Remote work will occur Monday – Friday, 8 a.m. – 6 p.m. US Eastern time.
- Approved on-site work will be performed Monday – Friday, 8 a.m. – 6 p.m. Customer's local time or similar daytime working hours.
- To simulate real-world threat actors, goal-based testing, such as Penetration Tests and Red Team Tests, can occur at any time, within the testing dates, at Sophos' discretion.
- Work performed outside of the hours listed above, as requested or required by Customer, will incur additional service charges.

2 Service Details

The subsections below contain details about the Service and how it will be initiated.

2.1 Service Initiation

The rules of engagement for the assessment are established during scheduling and kickoff sessions. Topics to be covered include the following:

- Goals and objectives for the assessment
- Definition of scope and validation of targets
- Rules of engagement, levels of effort, and risk acceptance
- Testing timelines and schedules
- Reporting requirements, timelines and milestones
- Key personnel, roles and responsibilities, and emergency planning
- Sophos source Internet Protocol ("IP") address ranges, and tools and techniques

- Mobile device platforms, applications, versions, and other relevant technical information

After completion of all staging tasks and the introductory meeting, Sophos will send a confirmation email to ensure agreement on these items.

A member of the Sophos' team will be involved between the kickoff call and the start of testing to aid the Customer in completing any pre-testing tasks. These tasks include collecting IP addresses / targets / scope, configuring any remote testing connectivity, and other mandatory pre-testing tasks.

2.2 Service Scope

The Mobile Application Security Assessment Service includes the following scope:

- Testing for iOS and Android
- Client and server testing
- Testing of the API used by the mobile application

Sophos will conduct a Mobile Application Security Assessment for the number of mobile applications defined in an Agreement.

Sophos will conduct one (1) remediation validation ("RV") for only the high- and critical-severity findings listed in the final report.

After primary test completion, Customer has ninety (90) days in which to remediate issues, schedule the RV, and have Sophos perform the RV. Customer must submit the RV request through email to the Sophos point of contact for the assessment within thirty (30) days of delivery of the final report or the RV is forfeited.

Note: Sophos only conducts RVs remotely, regardless of whether the assessment was conducted on-site.

2.3 Service Methodology

Sophos will perform the following tasks during the Service.

Test User Accounts

Multiple user accounts are required to test what authorized users may accomplish, usually two authenticated user roles.

- Unauthenticated (anonymous) user
  - Access restricted resources that usually require authentication
  - Gain access to authenticated privileges or a user account
  - View other user/account data
- Authorized user
  - Elevate privileges to access internal or sensitive content
  - View other user/account data
  - Add/modify/delete other account data
  - Existing access is appropriate based upon role

Mobile Security Best Practices Review

During this phase Sophos will examine the objectives to be met by the application as well as test directly through the user-interface. These two points of view often lead to the fastest and highest quality results. By reviewing how the developer's approach to accomplish the application objectives, risk decisions can

be evaluated. This step also allows for validation that the implementation matches the desired design. Testing will focus exclusively on application security and security related issues, rather than usability.

The consultant will install the mobile application on the desired hardware platform and/or in an emulator and commence testing. This level of testing seeks to perform a static analysis of the application as it sits on a device in order to discover if any coding or logic vulnerabilities exist within the application which may lead to inappropriate access, either by an ordinary user during the course of routine application use or by a malicious attacker. The types of undesired activities which are often discovered by this testing scenario include:

- Accessing personally identifiable information (PII) of other application users
- Elevation of user privileges
- Exposure of underlying application code

This first stage is performed with knowledge of the design and goals, but little or no knowledge of the code or supporting systems. If applicable to the application being assessed, testing activities may include:

- Application manipulation
- User Input fields
- Error handling
- Access control
- Multi-factor authentication
- Strong password requirements
- Application updates
- Tethered
- Over-the-air
- Handling transaction interruptions
- Connectivity loss
- Switching networks during transaction
- Incoming call
- Exiting the application

Mobile Application Security Assessment

This stage includes a detailed manual security testing and an in-depth analysis of the application running on a device, in an effort to expose vulnerabilities which are not apparent from end-user interface testing only. Although not required for testing, the consultant team can work collaboratively with stakeholders such as those from Development, Project Management, and other identified business groups, to examine the different functions of the mobile application. Although a number of findings can possibly result from this analysis, some common discoveries include:

- "Logic layer" vulnerabilities
- Identification of debug or backdoor functionality
- Identification of any gaps in best practices (bad APIs, managed cryptography provider APIs, creating Customer cryptography method, risky identity management APIs, global shared variables that contain sensitive information)
- Identification of poor error handling (are errors handled gracefully by a central API or are they one-off debug prints and leaks, is environment clean up and recovery properly handled upon failure detection)

- Insecure storage of credentials or authentication tokens
- Insecure application behavior during back-grounding which stores sensitive information on the device, as well as fails to properly log the customer out of the application
- Failure to properly handle invalid SSL/TLS certificates for encrypting communications

The Sophos testing methodology uses a combination of software emulation, software development environments, and actual hardware to perform the mobile application testing. Different techniques must be used on each platform to perform similar checks. This is due to the differences in the way each mobile platform operates. Sophos testing methodology includes top vulnerabilities from the Open Web Application Security Project (OWASP) Mobile Security Project, other proprietary and open vulnerability sources, and undisclosed vulnerabilities. Tasks that Sophos performs includes the following:

- Application emulation
- Use of debugging tools
- Use of network proxies
- Limited device and application forensics

Sophos will dynamically assess the application using both automated and manual analysis to discover issues specific to the given architecture and design of the mobile application. The following topics represent the types of items that are assessed:

- Access control
- Session management
- Least privilege access
- Inappropriate storage
- Does the application store data it shouldn't?
- Password
- Password hash
- Sensitive information
- Logs
- Keys
- Insecure storage
- How does the application store data it needs to store?
- Encrypted vs. clear text
- Cryptographic implementation
- Insecure transport layer
- Does Customer force SSL for all communications?
- How does Customer handle bad certificates?
- Does Customer implement SSL correctly?
- Other transport layer issues, such as IPsec and VPN
- Application buffer overflow and similar vulnerabilities
- Is there any debugging or test code left in the application?
- Mechanisms to prevent malicious in-app advertisements
- Data leakage
- Location
- Device ID
- Personal information
- IP address
- Geo-location
- Platform-specific testing
- Keystroke caching
- Screen shots
- Keychain or password storage
- SQLite data storage
- Cached files and data
- UIPasteBoard
- Backgrounding action
- Snapshots

2.4 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.4.1 Delivery Coordination

Sophos will provide coordination for the Service(s) with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics for people, processes, and tools as well as timeline and meeting facilitation.

The scope of delivery coordination includes the following:

- Develop delivery timeline with Customer and with Sophos personnel
- Work with Customer to identify and address issues or concerns that impact service delivery
- Periodic, high-level updates on progress
- Confirm delivery and procure project sign-off

Services will be delivered remotely from a secure location or, if an exception has been approved then from the Customer's site(s).

Sophos solely reserves the right to refuse to travel to locations deemed unsafe by Sophos or locations that would require a forced intellectual property transfer by Sophos. Sophos solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Sophos. Customer will be notified at the time that services are requested if Sophos refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Sophos travel is arranged. In the event any quarantines, restrictions, or measures imposed by governmental authority or Sophos restrict travel to any location, Sophos may at its election (i) deliver the Services remotely or (ii) postpone the Services until travel is permitted. If neither option (i) nor (ii) in the preceding sentence is feasible, Sophos may terminate the affected Services and provide Customer with a refund of any unused, prepaid fees.

3 Deliverables

Listed in the tables below are the standard deliverables for the Service. Sophos will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Mobile Application Security Testing	Final Report	Upon completion of testing	Email

3.1 Final Report

During the three (3) weeks after delivering the Service, the Sophos Technical Quality Assurance ("TQA") process for reporting may require validation and investigation of issues raised in the report. This will result in a small amount of testing outside the primary testing interval that will stop prior to delivery of the report. At the end of the TQA process, Sophos will issue a formal report to the Customer designated point of contact.

Customer shall have one (1) week from delivery of the report to provide comments to be included in the final report. If there are no comments received from Customer before expiration of the review period, the report will be deemed final.

Upon completion of the Service, the Customer-designated contact will receive a secure/encrypted email confirmation from Sophos. Unless otherwise notified in writing to the contrary by Customer designated contact, within five (5) business days of such email confirmation, the Service shall be deemed complete.

3.2 Out of Scope

The information in Section 2 comprises the Sophos standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Upon request, Sophos can provide out-of-scope technical support on a time and materials basis pursuant to a separate Agreement. Sophos reserves the right to decline requests that:

- Are beyond the scope of the Service(s) described herein
- Are beyond the capability of Sophos to deliver within the contracted service levels
- Might violate legal or regulatory requirements

4 Service Fees and Related Information

See Sophos applicable Agreement for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

4.1 Invoice Commencement

See the Service-specific Addendum incorporated herein by reference at https://www.sophos.com/legal/-terms, as updated from time to time (the “Product Terms Page”) or Agreement for information about invoice commencement. Provisions related to the term of the Service and payment terms within the Product Terms Page shall not apply to Customer’s consumption of Services in case of purchases through a Sophos’ reseller but instead shall be subject to Customer’s agreement with its reseller.

4.2 Expenses

Customer agrees to reimburse Sophos, directly or indirectly (in case of purchases through an authorized reseller), for all reasonable and actual expenses incurred in conjunction with delivery of the Service.

These expenses include but are not limited to the following:

- Travel fees related to transportation, meals, and lodging to perform the Services, including travel to Customer location(s)
- Digital media storage, specific equipment necessary for delivering the Service, or licensing necessary for tailored digital forensic analysis work.
- Monthly fees for other purchased infrastructure to support service delivery (e.g., public cloud computing services) may apply, if Customer and Sophos agree that usage is necessary to complete Service delivery.

4.3 Term

The term of the Service is defined in the Agreement. Service will expire according to the Agreement provided that, if there is currently an in-progress delivery of the Service at the time of expiration, then the term shall automatically extend and expire upon completion of such in-progress delivery of the Service. During such extended term (if applicable), the terms and conditions of the Agreement shall be in full force and effect.

5 Additional Terms

5.1 For Approved On-site Services

Notwithstanding Sophos' employees' placement at Customer's location(s), Sophos retains the right to control the work of such employees. For international travel, on-site Services may require additional documentation, such as visas, visitor invitations, and related documentation, which may affect timing of the Services and reimbursable expenses.

5.2 Security Services

Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding Customer's systems and accepts those risks and consequences. Customer hereby consents and authorizes Sophos to provide any or all of the Security Services with respect to Customer's systems. Customer further acknowledges that it is Customer's responsibility to restore network computer systems to a secure configuration after Sophos completes testing.

5.3 Record Retention

Sophos will retain a copy of the Customer Reports in accordance with Sophos' record retention policy. Unless Customer gives Sophos written notice to the contrary prior thereto and subject to the provisions of the applicable Agreement and DPA, all Customer Data collected during the Services and stored by Sophos will be deleted within 30 days from issuance of the final Customer Report. If Customer or its authorized agent requests that Sophos retain Customer Data for longer than its standard retention policy, Customer shall pay Sophos' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Sophos shall be entitled to retain Customer Data as necessary to comply with its own legal, regulatory, judicial, audit, or internal compliance requirements.

5.4 Compliance Services

Customer understands that, although Sophos' Services may discuss or relate to legal issues, Sophos does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Sophos in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

5.5 Post-Engagement Activities

Subject to any applicable legal or regulatory requirements, thirty (30) days after completing delivery of the Service, Sophos will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Sophos in the performance of the Services hereunder (the "**Engagement Media**"), unless prior to such commencement, Customer has specified in writing to Sophos any special requirements for Sophos to return such Engagement Media (at Customer's sole expense). Upon Customer's request, Sophos will provide options for the transfer to

Customer of Engagement Media and the related costs thereto. If so requested, Sophos will provide a confirmation letter to Customer addressing completion and scope of these post-engagement activities, in Sophos' standard form. Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Sophos shall, in its sole discretion, dispose of the Engagement Media on or after the engagement conclusion and only maintain a copy of the completed engagement-specific deliverables.

5.6 Legal Proceedings

If Customer knows or has reason to believe that Sophos or its employees performing Services under this Service have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require Sophos or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Sophos, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Sophos for (a) its employees' time spent as to such response, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and Sophos as to the Service.

5.7 Endpoint Assessment

Unless otherwise agreed upon in writing, if a software agent has been deployed as part of the Service, within thirty (30) days following the date of the Completed Final Report (the "Thirty Day Period"), Customer shall uninstall any and all copies of the software agent used for the Service. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Sophos' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Sophos from the software agent. Customer will uninstall the software agent as described in this Service.